Analysis of the bug

The `fopen` function creates files with r/w permissions for everyone, filtered by the process's umask. The umask, however, is inherited by the parent of the process which, for a setuid/setgid program, may be controlled by the attacker.